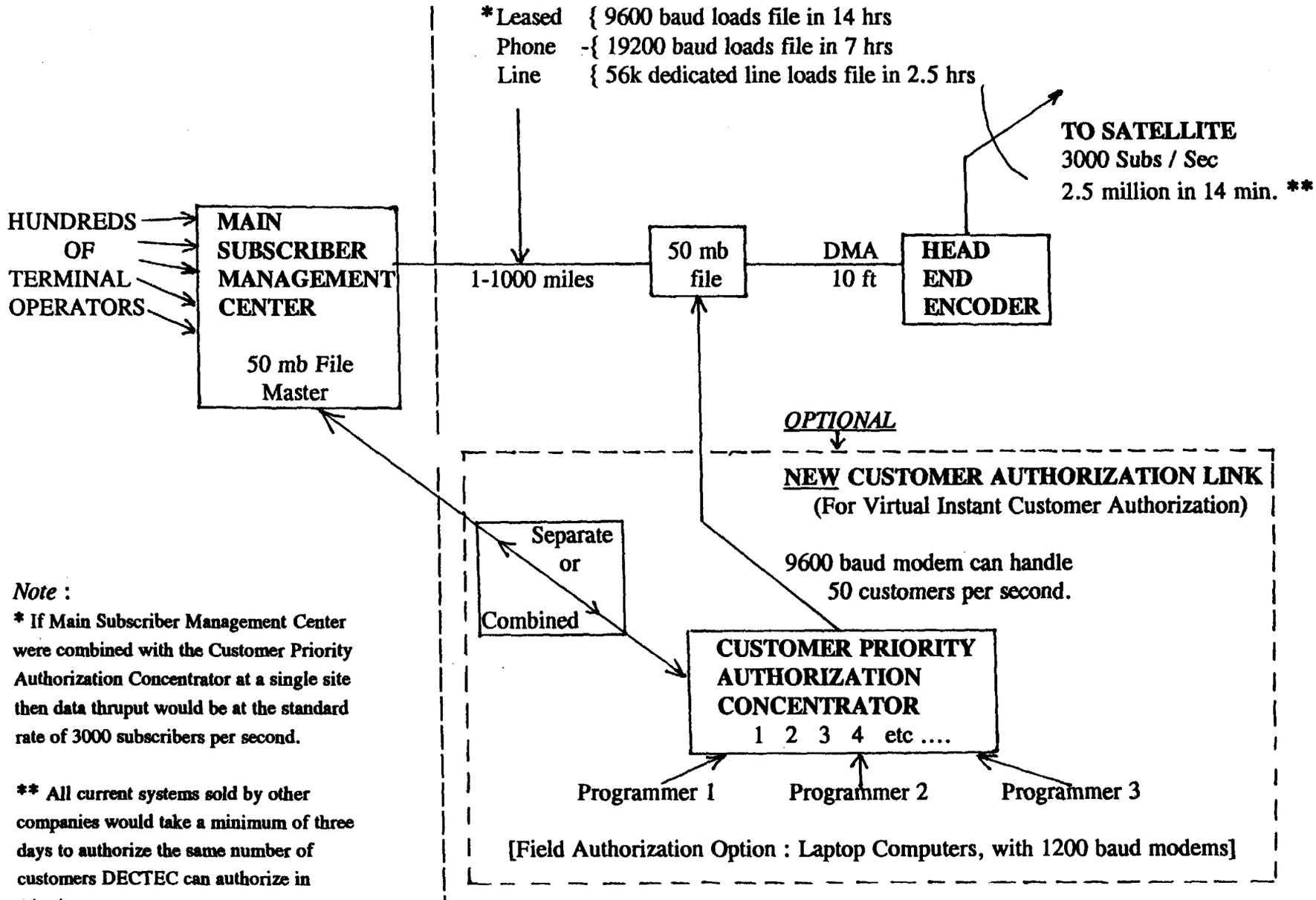
**SUBSCRIBER MANAGEMENT**

**SOURCE :** Supplied by any Third Party Existing Back Room Operation

**PRIMARY SYSTEM**

**SOURCE :** DECTEC UNIVERSAL TELEPORT, supplied by DECTEC.




*Note* :

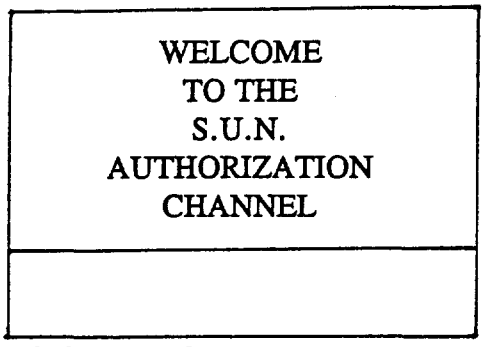
* If Main Subscriber Management Center were combined with the Customer Priority Authorization Concentrator at a single site then data thruput would be at the standard rate of 3000 subscribers per second.

** All current systems sold by other companies would take a minimum of three days to authorize the same number of customers DECTEC can authorize in 14 minutes.

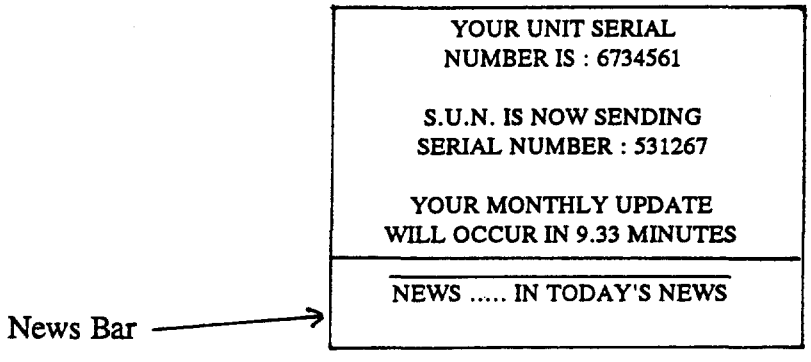
## TYPICAL CONSUMER FEATURES

a) *Customer Tunes to S.U.N. Authorization & Monthly Update Channel.*

This TV Screen appears

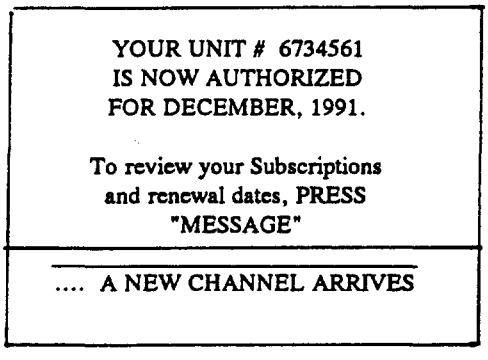



b) *This Display appears 5 seconds later on the customer's TV screen.*




The customer is now free to tune to another channel for approximately 9 minutes and then return to the S.U.N. Authorization Channel for his monthly update. Or the customer can tune to the Authorization Channel at bed time and leave it there over-nite. His satellite receiver and TV can be shut off while the authorization or monthly update takes place. However, each new customer authorization is typically instantaneous when the **Customer Priority Authorization Concentrator** is used.

c) *Third and final On-Screen Display, after new data has been recieved.*



SPECIAL NOTES :

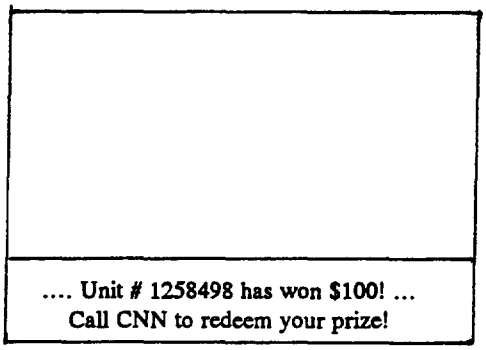
- the customer must "AUTHORIZE" his S.U.N. unit each and every month. This gives the Programmer complete control over the subscriber on a month to month basis.

- Typical S.U.N. **Monthly Update** Authorization time with 2.5 million active customers is less than 7 minutes.

## OPTIONAL FEATURES.

- Moving Information / News Bar at bottom of screen on S.U.N. Authorization Channel. This "Bar" could be used for :
  - a S.U.N. "Lottery"
  - Programming Promotions.

EG:




## P.P.V.

The DECTEC Universal Teleport is ideally suited for the rapid authorization of special and pay-per-view events.

# Customer Authorization via HBI using S.U.N. authorization data in standard mode:

## Data Rate

1 BYTE every 384 micro seconds
120 messages/second
100 customers/second
360,000 customers per hour
1 million customers in 3 hours
ADD
x3 data redundancy: 1 million customers addressed every 10 hours

## SYSTEM COST ANALYSIS

*Based on :*

2.5 million New Subscribers per year.

*You will then need to authorize ...*

50 thousand customers every 5 day week, *or,*

10 thousand customers every day.

At 5 minutes per authorization you require 833 person hours to authorize 10,000 customers each day.

*This equals to 100 phone operators per 8 hour day.*

## LABOUR & OVERHEAD COST

100 OPERATORS @ $12,000 per annum.

OVERHEAD @ $3000 per operator per annum.

$15,000 x 100 = Yearly Cost : $1.5 million.

Transponder & Technical Cost : $1 million.

Telephone Cost : $1.5 million (approximate)

*TOTAL COST / YEAR* : **$4 MILLION**

## PROJECTED COST OF SYSTEM (Per Year)

| | |
|---|---|
| 0 - 830,000 Subs | $2 million |
| 830,000 - 1.6 million Subs | $3 million |
| 1.6 - 2.5 million Subs | $4 million |

## REVENUE (Per Year)

*BREAKEVEN POINT* : 80,000 Subs @ $25 each, per annum = $2 million

| | Expenses | | Profit |
|---|---|---|---|
| 1/4 million Subs | $2 million | = | $4.25 million |
| 1/2 million Subs | $2 million | = | $10.5 million |
| 1 million Subs | $3 million | = | $22 million |
| 2 million Subs | $4 million | = | $46 million |
| 2.5 million Subs | $4 million | = | $58.5 million |

G

DECTEC INTERNATIONAL INC.
P.O. BOX 2275, SIDNEY, BRITISH COLUMBIA, V8L 3S8, CANADA
Offices: 1962 Mills Road Phone: (604) 655-4463 FAX: (604) 655-3906

October 1, 1989

Reiss Media Enterprises
240 Pegasus Ave.,
North Vale, NJ 07647
USA

Dear Sirs,

This letter is to clarify what we feel the situation currently is regarding the protected transmission of programming via the VCII system. In order that we understand each other and the problems involved, together with a proposed solution, we will, at the same time, present a bit of a VCII primer. Please bear with us if we seem to be, at times, re-stating the obvious.

There are basically two levels of protected service offered:

The first is a tiered service with a common working key useable on all the channels within the tiered system and the 'protection' preventing a subscriber to one channel watching programming on another channel being limited to a channel mask bit which is part of the decryption process within the 7001 CMOS micro used. This was adequate as long as the single chip micro code was inaccessable and had no bugs but this is not the case. Initially it could be broken by using loopholes in the code to bypass the bit mask check (original purple lable cages). The second generation (blue lable cages) were broken by generating an all pass channel mask externally by executing the DES algorithm in the main processor. The third generation (03 keys or grey cages) have been broken in two ways: firstly by a two stage process of external DES algorithm generation combined with a genuine subscription to one channel, typically CNN and secondly by replacing the single chip micro with another containing code with the mask check bypassed as in original cages. A further refinement is to bypass this single chip micro entirely, calculate the data within the main processor and send the result directly to the audio decryptor/ deserialiser set. The flaw basically is that to handle 50 odd channels, you must have a common key or you would need to send potentially 50 odd unique keys to subscribers which the system overhead with a million plus users simply could not sustain (and the current hardware could not handle either).

... 2

The second level of service is potentially capable of solving this shared key flaw by being offered to those users who only watch a single channel (typically a hotel or cable operator permanently tuned to one transponder). With only one channel involved, a unique key for that channel can be used which is unuseable on any other channel. This approach is reasonable unless cloning is considered or the use of Wizard keys. If any one of the legitimately subscribed commercial boxes out there is modified to display the working key used for that month and this information is disseminated to users with boxes capable of entering this number, then these users can watch too. Alternatively, if the seed keys of any of these boxes are extracted they can be used to provide clones which will also be able to watch. GI has tried a half hearted attempt to solve the first by changing the keys more than once a month, thus frustrating the dissemination of current key information, but did not continue the experiment for some reason. The use of cloned keys has been common on tiered systems in the past because there were so many thousands of them that if a few were discovered and shut down, there were many replacements. Up till now, no-one considered putting commercial seed keys in customer units as a means to watch these channels because of the relative scarcity of commercial users willing to jeopordise their own units. However this will change with the imminent introduction of cages modified with truly secure decryption chips in which one or more sets of IDs and associated seed keys can be stored with impunity.

The key then to breaking current VCII programming is the availability of the seed keys from legitimately subscribed units. If a single set of keys becomes available then this set can be used either by cloning or by the Wizard approach to activate other units. It is therefore essential that a new method of preserving these seed keys from scrutiny by anyone is achieved. This is what we have done. This same technology which makes it impossible for other dealers or GI themselves to read the keys of a modified unit (to copy it or shut it off) could equally be used to prevent pirates from reading these keys and using the cloning/wizard processes.

Our module is currently based on the Intel 8751 microcontroller with its security lockbits, a design which has been used for years extensively in banking machines without security problems. With some associated data capture logic, it bypasses the data recovery chip GI uses and handles the VCII data stream directly. In each 8751 are one (or more) sets of IDs and seed keys, for which a match is constantly being attempted for subscription information. Should a monthly set of subscription data be received for that units ID, it is stored and when it is needed, typically the next month, the result (movie key) is calculated internally and sent directly to the audio decryption/ deserialiser chip. There is no external indication of internal activity and both the seed keys and the ID itself are never referred to outside the 8751. Consequently, these IDs and seed keys are totally secure and form no basis for cloning or Wizard use.

In addition, because we handle the data stream directly, we are not limited to particular service IDs but can handle any and all simultaneously. It would therefore be perfectly feasible to supply modified cages with new seed keys operating on the current service ID which could be exchanged for existing customer units on a controlled but leisurely basis such that at some point in the future when all customers had received their new cages, a switch could be made to a new service ID which all the cages would respond to but which no other cages could work with. This involves two potential levels of co-operation by GI. Ideally, for each customer cage they would provide the seed keys for that ID to be put into the new cage. OR they could provide new seed keys to go with new IDs. It seems to us that possibly GI's own internal security might be questionable in which case it might make more sense for us to provide unique IDs and seed keys which GI would have to calculate new monthly codes for but this may be beyond their capabilities.

In summation, what we propose is a field trial with cages modified to include our modules and operating code. GI would have to agree to issue a new service ID at some point, preferably in parallel with current service IDs so that initially both systems would operate for testing. When everyone was satisfied that the modified units operated equally well on both old and new service IDs, the old service ID could be discontinued and only the modified cages would continue to run.

The problem we cannot solve is GI's willingness or otherwise to participate in helping you, when it is obvious to us that they have had the engineering ability to solve these problems earlier but decided not to do so because of the impact on their profits. Should they refuse point blank to be involved at all, the only solution we can see would be to have us design and build your own head end with your own customer subscription interface and your total control of the keys (and security) as you see fit. This could lead to legal problems in the use of what they may feel to be their system even if it uses a totally new protocal, but someone will have to stand behind the attempt, especially once it is obviously successful. In fairness, GI would still be selling their cages so could not logically complain but realistically the unavailability of 'pirateable' cages must inevitably eat heavily into their sales.

We stand ready to participate in building a system offering that much-hackneyed and abused phrase 'total security'. One final word of caution: someone, somewhere must generate the new monthly key to be used in all subscribed units. There is no point in having totally secure hardware if there is any possibility of this information leaking from the organization that generated it. Thus ideally each programmer would perform this task and the issue of security would be his own personal problem. It is only in recognition of the fact that there are so many units out there and so many services which customers still want to watch that we are forced to create a solution compatible with existing VCII technology rather than a separate solution. The latter could be provided as well.

... 4

One last thought: assuming the concept of unreadable keys and unbreakable boxes is eventually accepted albeit with much scepticism, there will no longer be a need to update everybody everymonth and so the system would be capable of handling new tiers, with each subscriber getting more than one set of monthly updates (if subscribed to more than one set of tiers). The hardware has sufficient RAM to accomodate dozens of 56 channel tiers right now; only the never used message handling area need be deleted. What we are stating for current tier users is that once the security problem is fixed there is no need to go to a VCII plus system to get additional channel space, the current system can handle it with only a change in run time EPROM. As well all existing VCII modules could be used for IPPV application with the capacity for hundreds of PPV channels. With our security module in place it would not be possible (as it is now) to fraudulently alter the number of credit dollars in each consumer's unit.

Minimum risk staged proposal:

Stage one: inform GI of the proposed solution and establish what their initial level of co-operation will be. Succeeding actions will depend on the response. Get them to provide on your channel(s) an additional service ID (preferably one current cages can't get) in parallel with the existing service ID and one set of commercial seed keys and associated monthly update and movie key data on that channel(s). We will then create one unit which can be demonstrated working on both old and new systems. If they refuse on principle to release a set of keys we will provide a unit ID and its seed keys in the full knowledge that they have the right to turn off this unit at the end of the experiment. This stage involves you and GI in no hardware purchase or modification but simply some software mods at the head end (which they have done for other commercial channels already and so cannot plead ignorance of). It will establish initially that the system would work as well as the existing system and give you confidence before committing all your subscribers to it.

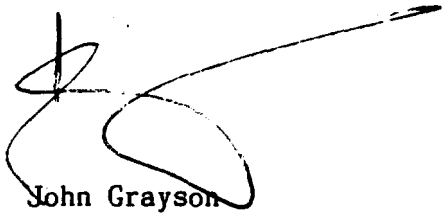
Stage two: Replace all existing customer cages with new ones, modified by us. At this point GI either has to provide the existing old seed keys or brand new ones.(If it is at your request it is hard to understand their objections because the only person who could be harmed by the leak of this information is yourself and it is certainly not in our interests to see this information leaked; if paranoia sets in, we could possibly allow you or GI to program the 8751s with our code and your seed keys and then set the security bits in our absence!) Once all cages had been shipped to the field and installed they could run on the old system until any bugs if any had been cleared up. Finally, on D-Day the old service ID transmissions could be terminated and the cages would continue to run on the new service ID.

... 5

Stage three: monitor the system for however long it takes to satisfy yourselves no unsubscribed party is taking your programming. We would be happy to be paid our engineering fee on the basis of a certain percentage for each month for which no break of the system is reported. Our only concern is that GI themselves might leak the information to destroy credibility.....

Stage four: tell all the other programmers that there IS a solution to their problems.

Sincerely,



John Grayson
C.E.O.
DECTEC INTERNATIONAL Inc.

c.c.: P. Resch - Disney

A draft of a proposed letter to be sent to:

DECTEC International Inc.,
1962 Mills Rd.,
P.O. Box 2275,
Sidney, BC V8L 3S3

Sirs:

In response to your proposal concerning our problems with the security of our satellite broadcasts, we are indeed interested in pursuing a solution based on your security module, in the staged experiment outlined. To implement stage one (single unit proof of concept) we will persuade GI to co-operate and issue an additional new service ID in parallel with the existing one on channel XXX. We will attempt to acquire one old set or one new set of seed keys or will accept your offer of a set read from an existing cage if this proves unworkable. We will then further request GI to send monthly update information for this unit and also the associated continuous movie key updates.

Should this single user unit be shown to operate in a consistent manner on both old and new service IDs in an acceptable manner, we will proceed to stage two and request the modifying of a set of cages to be provided by us to replace all our existing units on channel XXX. We will endeavour to solve the problem of loading seed keys into these units to GIs satisfaction, possibly involving the last resort of their loading of the Intel security chip with your code and their keys in our joint absence. Once all customers have the new units installed and operating in a satisfactory manner on the new ID we will request termination of the old ID.

If your signal security module system performs as proposed, we will inform other programmers of this option and, as well, of our satisfaction with your signal security system.

Sincerely,

H

Statement of

JAMES F. BUNKER

President, GENERAL INSTRUMENT - VIDEOCIPHER DIVISION

Past President, M/A-COM INC.

before the

Subcommittee on Telecommunications, Consumer Protection and

Finance Committee on Energy and Commerce

U.S. House of Representatives

March 6, 1986

Chairman Wirth and members of the subcommittee, my name is James F. Bunker and I am Senior Vice President of M/A-COM, Inc. I want to thank you for this opportunity to appear before you and describe M/A-COM's activities over the past several years in the field of video scrambling. In addition, I want you to know that we oppose H.R. 1769, H.R. 1840 and H.R. 3989, because they would result in unwarranted government intrusions into a vigorous and competitive marketplace.

M/A-COM is a major supplier of components, equipment and systems for commercial telecommunications and defense applications. Through our operating companies, we are a leading supplier of digital information processing and transmission equipment for satellite communications, data communications, fiber optics, television broadcast and CATV. We are the producer of the broadest range of microwave components for manufacturers of equipment used in the defense and commercial telecommunications market.

As our product line specifically relates to satellite video scrambling, we are a leading producer of data encryption equipment for both commercial and national security applications, we manufacture antennas for satellite earth stations, and also sell commercial and home satellite receivers. Thus, our participation in these areas provided a natural fit when the marketplace requirement for satellite video scrambling arose. This statement describes in more detail our participation in that market.

The Satellite Video Market

First, I want to point out that the satellite video marketplace is extremely complex, perhaps more complex than any other discrete marketplace within the grand category of telecommunications over which this subcommittee has jurisdiction. Here is a list of the most important players in the satellite video marketplace:

program producers (e.g., Hollywood studios)
program packagers/syndicators (e.g., HBO, Showtime)
cable TV operators
cable TV subscribers
home TV receive-only earth station (HTVRO) manufacturers
HTVRO wholesalers/distributors
HTVRO retailers
HTVRO owners
TV set manufacturers
commercial TV networks
trade associations (e.g., NCTA, SPACE)
domestic satellite owners/operators
Federal Communications Commission
Congress of the United States

When the Congress passed the 1984 cable TV legislation, some members of Congress felt that the public interest would be best served if satellite video programmers would provide service to the owners of HTVRO earth stations, employing scrambling as a way to protect access to the signals. My point in listing these players is to show that there are many competing interests, and that it has been a slow and difficult task to reach the marketplace accommodations that were necessary to let satellite video scrambling proceed. However, it is now going forward, and it is proceeding in a manner that does serve the public interest.

This marketplace is vigorously competitive. What we have seen, and continue to see, is the normal working of a competitive marketplace. M/A-COM believes that the free marketplace, free from government control, usually produces the best products and services at lowest costs for the American consumer. We oppose H.R. 1769, H.R. 1840 and H.R. 3989 because those bills would interfere with the free working of the marketplace and would penalize American consumers.

At this time satellite video scrambling is going forward, and we feel that the overall system concept is in the best interest of the consumer and the other parties with a significant interest. M/A-COM is proud to have participated in formulating that system concept.

Historical Review

To describe where we are today, it is necessary to review the development of the satellite video distribution industry over the last decade. Starting in the 1970s, Home Box Office and other program syndicators began distributing packages of movies and other entertainment to CATV systems using point-to-point terrestrial microwave. This use of point-to-point microwave relays gave complete control over access to the signals.

Later in the 1970s, HBO took the lead in the industry because it was the first to recognize that domestic satellites could be used to distribute video

to a wider range of CATV affiliates at a lower cost than terrestrial microwave. In the 1970s, receive-only earth stations cost upwards of $100,000, so that economic considerations resulted in nearly the same degree of control over access to the signal as had been the case with point-to-point microwave. The earth stations were simply too expensive to be owned by large numbers of consumers.

In the early 1980s, however, the trend to lower cost earth stations was becoming clear. As satellites were launched with higher power and the receiver technology matured, thousands and then tens of thousands of earth stations were sold to commercial establishments and private consumers.

It was at this point that HBO and other satellite programmers became concerned about limiting access to their signals, particularly with respect to the commercial establishments. Some of these programmers felt that their signals were protected from unauthorized private viewing by Section 605 of the Communications Act, since they were not using the satellites to "broadcast" but rather to distribute their signals to discrete locations. However, they also felt that it would be difficult, expensive and perhaps politically impossible to try to enforce the protection of intellectual property rights guaranteed by Section 605 with respect to private HTVRO owners.

Consequently, to a large extent the interest in satellite video scrambling was an economically-driven technological alternative to court enforcement of intellectual property rights. I want to stress the influence of economics

in the decision processes, because economics has continued to play a very influential role as the scrambling system design evolved.

In 1982, HBO became the first satellite video programmer to move in the direction of video scrambling by releasing a Request for Proposals for a video scrambling system. M/A-COM and other telecommunications equipment manufacturers responded to this competitive RFP, and M/A-COM won the competition. The winning design included digital encryption of the audio, very secure digital processing of the video signal, and an array of administrative features that were necessary for the commercial aspects of the system. Among the administrative features were the ability to directly address and authorize individual descramblers. This system is now known as VideoCipher(R) I.

However, during 1983, as we went from the design to the prototype and pre-production stage, it became clear that the VideoCipher(R) I design was too expensive for delivery to a consumer market in the 1985 time frame, because of the extensive digital processing of the video signal. This made it unacceptable to HBO, because by 1983 HBO had apparently decided that the consumer market was important and could not be ignored.

Consequently, M/A-COM redesigned the system so that it could be produced at substantially lower cost. This new system design, now known as VideoCipher(R) II, retains the digital encryption of the audio but substitutes a somewhat less secure but lower cost analog scrambling technique for the video.

In addition, during this period the administrative capabilities were enhanced so that competing program suppliers could use our system and the consumer would only need to buy a single descrambler. We felt, and we continue to feel, that this is an important feature of our system. We do not believe that the public interest would be served by the adoption of several incompatible scrambling techniques that would require consumers to buy several different pieces of hardware if they wanted to to subscribe to several different program suppliers. We did not want a situation to arise that was similar to the VHS-Beta incompatibility in the video recorder market, so we designed our system to accommodate all programmers that wanted to scramble their signals. In this way, competition between programmers will occur in the programming marketplace, and it will not be distorted by limitations designed into the hardware.

By March of 1984, the VideoCipher(R) II system design was virtually completed, and in October we released the preliminary interface specifications, first to HBO and then to HTVRO manufacturers. Since the descrambler must be connected between the outside dish antenna and the indoor HTVRO receiver, it was important both for the HTVRO manufacturers to understand the electrical specifications of our descrambler and for us to understand the electrical specifications of their receivers.

We had hoped that the receiver manufacturers would supply us with information about their units, but when this did not occur we went out to

retailers and purchased them. Between M/A-COM and HBO, we purchased and tested over thirty different HTVRO receivers to test for compatibility. Our initial design goal was to make our descrambler compatible with over fifty percent of the HTVRO receivers on the market. Later, at the programmers' urging, we changed this goal to ninety percent compatibility and we revised our design accordingly.

Throughout 1984, we were continuing to discuss video scrambling with other satellite video programmers, but no other programmers were willing to make a commitment to scramble at that time. Moreover, several of our competitors were actively marketing video scrambling systems that were incompatible with our design.

Finally, in November 1984 we signed a contract to provide scrambling and descrambling equipment to Showtime/The Movie Channel. This decision was the next important step that eventually led to adoption of VideoCipher(R) II as the de facto industry standard. However, our competitors continued to try to market their systems to the undecided programmers. The majority of the programmers held back on their decision to scramble and choice of a scrambling system until the second half of 1985.

In October 1984, we began delivery of the uplink scrambling equipment to HBO and by March 1985 we had completed delivery of cable headend descramblers to the cable TV systems that were affiliates of HBO. HBO began testing the system gradually, initially scrambling a few hours of programming per week.

By late 1985, as much as half of the HBO programming was being scrambled on a test basis.

During this testing program, we carefully monitored the reliability of the descramblers. By October 1985, over 46 million operational hours had been logged, with a mean time between failures of over 93 thousand hours, or about ten years. These descramblers are highly reliable, and we expect the consumer descramblers to be as reliable because much of the circuitry is identical.

Meanwhile, our efforts to work cooperatively with the HTVRO manufacturers continued. In March 1985, we hosted a meeting of over thirty HTVRO manufacturers where we explained the VideoCipher(R) II system in great detail. We spent time describing the interface specifications for the VideoCipher(R) II descrambler that is intended to retrofit existing HTVRO installations.

We also described in detail the specifications of the VideoCipher(R) II circuit module that is designed to fit into the next generation of HTVRO receivers. It is our hope that, starting around June 1986, the next generation of HTVRO receivers will be available that will incorporate the VideoCipher(R) II circuitry as a plug-in module comparable to a videotape cartridge. This will result in lower total cost to consumers and higher reliability.

Under the terms of our contracts with HBO and Showtime, we are committed to distribute our VideoCipher(R) II technology as widely as possible and make it available in modular form to fit into the HTVRO receivers made by other manufacturers. We are committed to making the technology widely available. Another aspect of our contracts, which I will discuss in more detail later, requires us to license second-source manufacturers of the descrambler modules.

During 1985, several additional events of note occurred. In May, we announced plans to operate the authorization computer center for the system on a non-profit basis. This computer center will receive the subscriber authorization information from each programmer, merge the information into a single data stream, and return that data stream to each programmer. In this way, a subscriber needs only to tune to any of the scrambled channels in order to be authorized to watch all that he has subscribed to.

This is a key public interest point that needs additional explanation. The system could have been designed so that each video signal would carry its own authorization information, but only its own. In this case, a subscriber would have to tune to each signal sometime during the month in order to receive the authorization for the next month. It is possible to conceive of a situation where a viewer finds nothing of interest on a particular program service during some particular month, so never tunes to that service and never receives the authorization information for the next month. If this were to occur, the viewer would be inconvenienced by having to make a telephone call

to the programmer to have a special authorization message sent. Our system design avoids that inconvenience.

Also in May, HBO announced that it would use the services of this authorization center. Our system is designed so that a programmer could, if it wished, operate its own authorization computer center separately from other programmers. However, our view was that consumers would be best served by the operation of a single authorization center in which all programmers participate. We are pleased to report that all of the programmers that have decided to scramble with the VideoCipher(R) II system have chosen also to participate in the single authorization center. That computer has been up and operating since January, at our facility in San Diego.

In the summer of 1985, we announced that we were ready to accept orders for consumer descramblers from wholesalers, distributors and HTVRO manufacturers. The initial order came from Channel Master, which is marketing a private label version of the descrambler.

Also in the summer of 1985, RCA endorsed the VideoCipher(R) II system. RCA's decision was largely based on the direct compatibility of VideoCipher(R) II with the 150 million TV sets now in American homes. VideoCipher(R) II uses a signal format known as NTSC, which stands for National Televsion Standards Committee; this is the industry committee that proposed the current TV format many years ago. In making this endorsement,

RCA rejected the alternative scrambling system based on a MAC (Multiplexed Analog Components) format.

During the September and October timeframe, a large number of programmers made decisions to scramble using M/A-COM's VideoCipher(R) II system. First, Showtime announced firm plans to begin offering scrambled programming to HTVRO owners, to begin May 1, 1986. Showtime also announced that it would participate in the use of the authorization center that M/A-COM is operating.

Then, Cable News Network--CNN1 and CNN2--announced plans to scramble and use the authorization center, to begin July 1, 1986. Since then, most of the other programmers--Disney, MTV, VH1, Nickelodeon, USA Network, and several new pay-per-view operators--have also announced plans to scramble during 1986, using VideoCipher(R) II technology and the authorization center in San Diego.

The last major event that took place occurred January 15, 1986, when HBO began scrambling all of its satellite feeds full time. It went off without a hitch. Although there was some press coverage of the event, it went largely unremarked outside the satellite video world.

With that as a historical review of the events that led us to where we are today, I now want to go over M/A-COM's equipment manufacturing and distribution plans in more detail.